

SYSTEM ACCESS NOMINATION AND AUTHORIZATION REQUEST (SANAR)**Army Civilian Personnel Systems****Privacy Act Statement**

AUTHORITY: Public Law 99-474, the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, authorizes collection of this information.

PURPOSE AND USE: The information will be used to verify that you are an authorized user of a U.S. Department of the Army civilian personnel automated information system (AIS) and/or to verify completion of your government personnel security investigation. Although disclosure of the information is voluntary, failure to provide the information may impede or prevent the processing of your SANAR.

DISCLOSURE: Disclosure of records of the information contained therein may be specifically disclosed outside the Department of Defense (DOD) according to the Blanket Routine Uses set at the beginning of the compilation of systems of records, published annually in the Federal Register, and the disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act.

PART I (To be completed by the Nominee for access [i.e., by the User] with Information Assurance Officer assistance.)

1. User ID (If known or already established):

2. Submission Date:

3. Name (Last, First, Middle, Title or Rank):

4. Expiration Date (for access requirement):

5. Action or Access Required (Continue on separate sheet if needed and identify attachments, if any.):

Complete the Items 6 through 11 below only if this is an initial request for an account or if the information previously provided has changed.

6. Social Security Number:

7. Date of Birth:

8. Phone (DSN):
(Commercial):

9. IP Address (or address range):

10. Mailing Address (duty):

11. E-Mail Address:

12. STATEMENT OF ACCOUNTABILITY: I understand my obligation to protect my password. I assume responsibility for the data and system to which I am granted access, in accordance with applicable policy and guidance. I will not exceed my authorized access, and will report changes in my need to know authorization, employment or duty status, or security status immediately to my Information Assurance Security Officer (IASO). I have completed security training and have read, signed, and agreed to comply with provisions of the *Security Features User's Guide (SFUG)* for the systems requested.

Nominee's Signature:

X

Date:

PART II (To be completed by Federal government Supervisor or Manager of the Nominee or User.)13. Sensitivity of Duties that Require Access (*Sensitive designation is reserved for certain security, system administration, and maintenance duties.*):☐ **NONSENSITIVE** or **SENSITIVE:** ☐ **ADP II** (Noncritical-sensitive) ☐ **ADP I** (Critical-sensitive)

14. Organization:

15. Supervisor's Name and Title:

16. Supervisor's Phone:

17. VERIFICATION OF NEED TO KNOW: (*The verifier of need to know must be a government employee: the supervisor, for a government employed nominee; or the Federal government manager or sponsor, for a non-government-employed nominee.*)

I have reviewed the information contained in this request. I certify that this nominee requires access as requested in the performance of his/her job function. I also certify the designation of this nominee's ADP position sensitivity, in accordance with AR 380-67 and AR 380-19, and compliance with citizenship provisions identified in those regulations for sensitive (ADP II and ADP I) positions. I will assure that changes in this nominee's need to know authorization, duty or employment status, or security status are promptly reported to the nominee's IASO.

Supervisor's Signature:

X

Date:

PART III (To be completed by nominee's Security Manager, and is required only if this requests initial issuance of the account, the previously reported investigation status has changed or expired, or the sensitivity reported in Item 13 has increased.)18. Investigation Type and Status (*NACI, BI, SBI, etc.*):

19. Investigation Completion Date:

20. Security Manager's Name:

21. Security Manager's Phone:

22. INVESTIGATION VERIFICATION: (*The verifier of the security investigation must be authorized by the government to verify this information, either as duties assigned to a Federal position or under provisions of a contract with the government.*)

I verify that the nominee has been subject of a favorably adjudicated personnel security investigation, which meets the position sensitivity requirements (stated in DoDD 5200.2, *DoD Personnel Security Program*, 9 April 1999) for the sensitivity indicated in Item 13, and which has not expired.

Security Manager's Signature:

X

Date:

PART IV (To be completed by nominee's organization Information Assurance Security Officer.)

23. Organization IASO's Name:

24. Organization IASO's Phone:

25. Organization IASO's E-mail:

26. ORGANIZATION IASO APPROVAL: I have reviewed this request and assure that the responsible individuals have correctly completed their respective parts and the nominee has received initial training in secure and appropriate use of the account. I will ensure that the nominee receives annual security training, monitor the security status of the nominee and account, and promptly report all incidents and changes to the designated installation IASO or Information Assurance Manager.

Organization IASO's Signature: **X**

Date:

INSTRUCTIONS

General Note on Usage: The System Access Nomination and Authorization Request (SANAR), SAMR-CP-PS Form 1, is available as an automated input form, which an originator can fill in using Microsoft Word. Though originators may print and manually fill it in, they are highly encouraged to use the automated version to fill in the required information. The originator (usually the nominee for access) should consult the appropriate sources and fill in all requested information, then print the signature-ready form.

Overview: The SANAR is used to nominate an individual for access to an access-controlled Department of the Army civilian personnel automated information system (AIS). It also is used to initiate changes to and deletions of access. The Designated Approving Authority, with jurisdiction over automated information systems that support Army-wide civilian personnel processes, has mandated its use for these systems. Separate instructions, which provide detailed instruction for each numbered item, and for processing the SANAR, are available.

Steps for requesting access or access related action:

1. Nominee (complete and sign Part 1). If you are a nominee for access, enter the indicated information to identify who and where you are, and what action or access you need. If you have already been issued a user-ID, enter that in *Item 1*. Otherwise leave *Item 1* blank. Describe the access required in full detail in *Item 5*. Use and attach additional sheet(s) if needed. Make note of any attachment(s) in *Item 5*. Consult application specific guidance and attach supplemental sheets if directed. Sign the statement of accountability and forward the form to the next recipient.

2. Supervisor (complete and sign Part 2). If you provide Federal government supervision or management of the nominee for access, you need to validate that the requested action or access is needed for performance of duties for the Federal government. Also, ensure that the sensitivity of the duties, for which access is requested, is correctly identified in *Item 13*. Note that the nominee's Information Assurance Security Officer (IASO) may waive the requirement for the supervisor's signature if the nominee is a high-grade government employee (GS-15 or O-6 or higher) and the IASO can function instead of the supervisor, in the manner described the detailed instructions.

3. Security Manager (complete and sign Part 3). If you are the security manager of the nominee for access, you need to provide the status of the nominee's personnel security investigation. You also need to verify that this satisfies requirements applicable to the sensitivity of the duties (identified in Part 2) and that any applicable citizenship-related requirements are met.

4. Information Assurance Security Officer (complete and sign Part 4). If you are the IASO of the nominee for access, you need to review the request for correctness and completeness. You need to assure that the nominee has received information security awareness training and that you will ensure notification, to the system IASO, of future events and status changes the effect the security of the access to be granted. You need to sign valid requests and forward these through information assurance channels, designated by your commander, to the system IASO.

The SANAR supports account management for Sensitive But Unclassified (SBU) Army civilian personnel AIS. It should not be used to support access to a classified AIS.

Questions regarding use of this form to support account management for an Army civilian personnel AIS should be addressed to the account manager for the AIS to be accessed. Issues not addressed at the account manager level should be elevated to ATTN: Information Assurance Manager, Office of the Assistant Secretary of the Army (Manpower and Reserve Affairs), Program Support Division, Civilian Personnel Systems Management Branch, 200 Stovall Street, Alexandria, VA 22332-0300. Phone numbers are commercial (703) 325-9415 and DSN 221-9415.